Google eliminó recientemente 106 extensiones de Chrome Web Store luego de descubrir que recopilan de forma ilegal los datos confidenciales de usuarios como parte de una *«campaña de vigilancia global masiva»* dirigida a los sectores de petróleo y gas, finanzas y atención médica.

Awake Security reveló los hallazgos el fin de semana, asegurando que los complementos del navegador web estaban vinculados a un único registrador de dominios de Internet, GalComm. Sin embargo, no está claro quién está detrás de la campaña de espionaje.

> *«Esta campaña y las extensiones de Chrome involucraron operaciones como tomar capturas de pantalla del dispositivo víctima, cargar malware, leer portapapeles y recolectar activamente tokens y comentarios de los usuarios»,* dijo Awake Security.

Las extensiones en cuestión se presentan como utilidades que ofrecen capacidades para convertir archivos de un formato a otro, entre otras herramientas para una navegación segura, al mismo tiempo que se basan en miles de revisiones falsas para engañar a los usuarios desprevenidos para que los instalen.

Además, los actores detrás de la operación aprovecharon las técnicas de evasión para evitar marcar los dominios como maliciosos con soluciones antimalware, permitiendo así que la campaña de vigilancia no sea detectada.

En total, las extensiones fueron descargadas casi 33 millones de veces en el transcurso de tres meses antes de que Awake Security se comunicara con Google en mayo.

Como respuesta a esto, Google desactivó las extensiones problemáticas del navegador. Se puede acceder a la lista completa de ID de extensiones ofensivas aquí.

Los datos de telemetría revelaron que algunas de las extensiones estaban activas en las redes de *«servicios financieros, petróleo y gas, medios y entretenimiento, atención médica y farmacéutica, comercio minorista, alta tecnología, educación superior y organizaciones*

gubernamentales», aunque no existe evidencia de que en realidad se usaron para recopilar datos confidenciales.

> *«Galcomm no está involucrado, y no está en complicidad con ninguna actividad maliciosa»,* dijo a Reuters el propietario del registrador con sede en Israel, Moshe Fogel.

Las extensiones en Chrome Web Store han seguido siendo un problema, ya que los malos actores lo explotan para publicidad maliciosa y otras campañas de robo de datos.

A inicios de febrero, Google eliminó 500 extensiones con malware después de ser descubiertas propagando adware y enviando la actividad de navegación de los usuarios a servidores controlados por atacantes. Después, en abril, la compañía eliminó otras 49 extensiones que se hicieron pasar por billeteras de criptomonedas para robar información de Keystore.